

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) UNCLASSIFIED REPORT.—

(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3078; amended Pub. L. 114–113, div. N, title II, § 229(b), Dec. 18, 2015, 129 Stat. 2974.)

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3534 and 3544 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2015—Subsec. (a)(1)(B)(v). Pub. L. 114–113 added cl. (v).

MAJOR INCIDENT

Pub. L. 113–283, §2(b), Dec. 18, 2014, 128 Stat. 3085, provided that: “The Director of the Office of Management and Budget shall—

“(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

“(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.”

§ 3555. Annual independent evaluation

(a) IN GENERAL.—(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;

(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems.

(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

(2) The Director’s report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with

the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

- (1) the adequacy and effectiveness of agency information security policies and practices; and
- (2) implementation of the requirements of this subchapter.

(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

(j) GUIDANCE.—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3082.)

REFERENCES IN TEXT

The Inspector General Act of 1978, referred to in subsec. (b)(1), is Pub. L. 95–452, Oct. 12, 1978, 92 Stat. 1101, which is set out in the Appendix to Title 5, Government Organization and Employees.

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3535 and 3545 of this title prior to repeal by Pub. L. 113–283.

§ 3556. Federal information security incident center

(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to—

- (1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
- (2) compile and analyze information about incidents that threaten information security;
- (3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;
- (4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and
- (5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national se-

curity systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

PRIOR PROVISIONS

Provisions similar to this section were contained in section 3546 of this title prior to repeal by Pub. L. 113–283.

§ 3557. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

- (1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- (2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
- (3) complies with the requirements of this subchapter.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3536 and 3547 of this title prior to repeal by Pub. L. 113–283.

§ 3558. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards¹ and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters² 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the

¹So in original. Probably should be “National Institute of Standards”.

²So in original. Probably should be “chapter”.